# Data Security and Protection Toolkit Assessment Summary Report 2020/21 (Final)

Walton Centre NHS Foundation Trust

Report Ref: 108WCFT_2021_902

Date of Issue: June 2021

# Contents



## Limitations

The matters raised in this report are only those which came to our attention during our internal audit work and are not necessarily a comprehensive statement of all the weaknesses that exist, or of all the improvements that may be required. Whilst every care has been taken to ensure that the information in this report is as accurate as possible, based on the information provided and documentation reviewed, no complete guarantee or warranty can be given with regards to the advice and information contained herein. Our work does not provide absolute assurance that material errors, loss or fraud do not exist.

Responsibility for a sound system of internal controls and the prevention and detection of fraud and other irregularities rests with management and work performed by internal audit should not be relied upon to identify all strengths and weaknesses in internal controls, nor relied upon to identify all circumstances of fraud or irregularity. Effective and timely implementation of our recommendations by management is important for the maintenance of a reliable internal control system.

Reports prepared by MIAA are prepared for your sole use and no responsibility is taken by MIAA or the auditors to any director or officer in their individual capacity. No responsibility to any third party is accepted as the report has not been prepared for, and is not intended for, any other purpose and a person who is not a party to the agreement for the provision of Internal Audit and shall not have any rights under the Contracts (Rights of Third Parties) Act 1999.

### Future periods

The assessment of controls relating to the process is that at June 2021. Historic evaluation of effectiveness is not always relevant to future periods due to the risk that:

- The design of controls may become inadequate because of changes in the operating environment, law, regulation or other; or
- The degree of compliance with policies and procedures may deteriorate.

## Public Sector Internal Audit Standards

Our work was completed in accordance with Public Sector Internal Audit Standards.

## Key Dates

| Report Stage | Date |
|---|---|
| Discussion Document Issued | 28/06/2021 |
| Final Draft Report Issued | 01/07/2021 |
| Client Approval Received | 08/07/2021 |
| Final Report Issued | 07/07/2021 |

## Report Distribution

| Name | Title |
|---|---|
| Mike Burns | Director of Finance & IT (SIRO) |
| Andy Nicolson | Medical Director (Caldicott Guardian) |
| Justin Griffiths | Head of IM&T |
| Lorraine Blyth | Digital Health Records & IG Manager |

## Audit Team

| Name | Contact Details | |
|---|---|---|
| Michael McCarthy | Michael.McCarthy@miaa.nhs.uk | 07552 258 920 |
| Gemma Owens | Gemma.Owens@miaa.nhs.uk | 07717 720 389 |
| Paula Fagan | Paula.Fagan@miaa.nhs.uk | 07825 592 866 |

## Acknowledgement and Further Information

MIAA would like to thank all staff for their co-operation and assistance in completing this review. This report has been prepared as commissioned by the organisation, and is for your sole use. If you have any queries regarding this review please contact the Audit Manager. To discuss any other issues then please contact the Director. MIAA would be grateful if you could complete a short survey using the link below to provide us with valuable feedback to support us in continuing to provide the best service to you.
https://www.surveymonkey.com/r/MIAA_Client_Feedback_Survey

# 1 Introduction, Background and Objective

In 2018 the Information Governance toolkit (IGT) was withdrawn and replaced with the new Data Security and Protection Toolkit (DSPT). It was developed by NHS Digital in response to The National Data Guardian's Review of Data Security, Consent and Opt-Outs published in July 2016 and the subsequent Government response, Your Data: Better Security, Better Choice, Better Care, published in July 2017.

The DSPT is a tool which allows organisations to measure their compliance against legislation and central guidance, and helps identify areas of full, partial or non-compliance.

In September 2020, NHS Digital published a methodology for independent assessment and internal audit providers to implement when performing DSPT audits (https://www.dsptoolkit.nhs.uk/News/83) which included a set scope for the review.

The published assessment methodology requires assessors/auditors to form a view on the in-scope assertions and key elements of your DSP Toolkit environment including:

- An assessment of the overall risk associated with the organisation's data security and data protection control environment. i.e. the level of risk associated with controls failing and data security and protection objectives not being achieved;
- An assessment as to the veracity of the organisation's self-assessment / DSP Toolkit submission and the assessor's level of confidence that the submission aligns to their assessment of the risk and controls.

The guidance also provides a reporting and scoring standard.

Whilst this guidance has formed the basis of our approach, we have had to apply flexibility and pragmatism to the approach given the impacts and challenges of delivering this review during the height of the third wave of coronavirus pandemic. As such, review and assessment in some instances has been based on evidence as provided rather than that independently obtained.

## 2 Scope

In accordance with the guidance mandated by NHS Digital, the selected thirteen DSPT assertions assessed during this review were:

| Area | Description |
|---|---|
| 1.6 | The use of personal information is subject to data protection by design and by default. |
| 1.8 | There is a clear understanding and management of the identified and significant risks to sensitive information and services |
| 2.2 | Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards. |
| 3.1 | There has been an assessment of data security and protection training needs across the organisation. |
| 4.2 | Organisation assures good management and maintenance of identity and access control for its networks and information systems |
| 5.1 | Process reviews are held at least once per year where data security is put at risk and following data security incidents. |
| 6.2 | All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway. |
| 7.2 | There is an effective test of the continuity plan and disaster recovery plan for data security incidents. |
| 7.3 | You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions. |
| 8.3 | Supported systems are kept up-to-date with the latest security patches. |
| 8.4 | You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service. |
| 9.2 | A penetration test has been scoped and undertaken |

| Area | Description |
|---|---|
| 10.2 | Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS Digital guidance. |

The scope of this review included only the mandatory elements of the above selected assertions.

# 3 Executive Summary

In the first year of the DSPT, 2018/19, the Trust met the standards. In 2019/20, the Trust again submitted a Standards Met assessment.

The Trust has demonstrated that it has plans for completion of its toolkit submission in time for the June 2021 submission including reporting of its baseline position

## 3.1 Areas of good practice

During our review we noted the following areas of good practice:

- The Trust had evidence of data protection by design audits being undertaken during the year under review.
- There was a Risk Management Policy in operation at the Trust which included the management of Information Governance and IT risks.
- The Trust could evidence a training needs analysis was in place during 2020-21 which included all staff and specialist IG role training requirements.
- There was evidence of ongoing monitoring of the Trust's IT estate in respect of anti-virus installation and patch management.
- Domain-based Message Authentication Reporting Conformance (DMARC) was enforced on the organisations email system.
- Testing on a sample of CareCERTs found that each had been remedied within 14 days of publication from NHS Digital.
- The Trust have recently reimplemented an offline backup solution for critical systems including EPR, PAS and pathology however it is noted that these arrangements should be formally risk assessed to ensure they provide appropriate protection to Trust data in the event of a ransomware attack.

## 3.2 Areas of vulnerability and/or where improvement is required

Our detailed findings and recommendations are described in more detail in a spreadsheet that has been provided under separate cover in order that vulnerabilities are not described in detail within this document. The spreadsheet should be treated as confidential as disclosure, without significant redaction, may result in any vulnerabilities becoming more widely known and exploited.

The key areas identified, however, can be summarised thus:

- During sample testing on user account access for terminations, it was identified that one account remained active and we were informed this was a decision by the IT team due to the importance of the ex-employee's role until a replacement was appointed. We were not provided any further evidence of assurance the Trust had that the ex-employee did not retain access to their account following their termination date.
- The Trust had not formally documented its controls in relation to web proxy and data loss prevention.
- The Vulnerability Management Policy could be strengthened to document the Trust's anti-virus processes in relation to managing alerts.

- It was found that there were no Recovery Time Objectives (RTOs) or Recovery Point Objectives (RPOs) agreed with system owners across the Trust.
- The Trust relies on virtual patching for out of support operating systems, such as Windows Server 2008. Whilst it is noted this does mitigate some risk, removal of end of support operating systems would be more secure.
- The Trust did not have a documented process for the monitoring of supplier certifications following onboarding.

# 4 Assessment and Assurance

## 4.1 Assessment of self-assessment

In our view, the organisation's self-assessment against the Toolkit deviates only minimally from the Independent Assessment and, as such, the assurance level in respect of the veracity of the self-assessment is:

| Substantial |
|---|

## 4.2 Assessment against National Data Guardian Standards

Across the National Data Guardian Standards our assurance ratings, based upon criteria at Appendix B are:

| National Data Guardian Standard level | Overall assurance rating at the National Data Guardian level |
|---|---|
| 1. Personal Confidential Data | Substantial |
| 2. Staff Responsibilities | Substantial |
| 3. Training | Substantial |
| 4. Managing Data Access | Substantial |
| 5. Process Reviews | Substantial |
| 6. Responding to Incidents | Substantial |
| 7. Continuity Planning | Substantial |
| 8. Unsupported Systems | Substantial |
| 9. IT Protection | Substantial |
| 10. Accountable Suppliers | Substantial |

The rating is based on a mean risk rating score at the National Data Guardian (NDG) standard level. Scores have been calculated using the guidance from the independent assessment Guidance document.

As a result of the above, our overall assurance level across all 10 NDG Standards is rated as:

| Substantial |
|---|

## Appendix A: Terms of Reference

Our work aimed to assess and provide assurance based upon the validity of the organisation's intended final submission, and consider not only if the submission is reasonable based on the evidence submitted, but also provide assurance based on the extent to which information risk has been managed in this context.

Our scope was based on that recommended as part of the Data Security and Protection (DSP) Toolkit Strengthening Assurance Guide published in 2020 by NHS Digital. As such our assessment involved the following steps:

- Obtain access to your organisation's DSP Toolkit self-assessment.
- Discuss the mandatory assertions that will be assessed with your organisation and define the evidence texts that will be examined during the assessment.
- Request and review the documentation provided in relation to evidence texts that are in scope of this assessment prior to the audit (if applicable).
- Interviewing the relevant stakeholders as directed by the organisation lead, who are responsible for each of the assertion evidence texts/self-assessment responses or people, processes and technology.
- Review the operation of key technical controls on-site using the DSP Toolkit Independent Assessment Framework as well as exercising professional judgement and knowledge of the organisation being assessed.

### Selected Assertions

As based on the recommended scoping from NHS digital the selected thirteen assertions are as follows:

| Area | Description |
|---|---|
| 1.6 | The use of personal information is subject to data protection by design and by default. |
| 1.8 | There is a clear understanding and management of the identified and significant risks to sensitive information and services |
| 2.2 | Staff are supported in understanding their obligations under the National Data Guardian's Data Security Standards. |

| Area | Description |
|---|---|
| 3.1 | There has been an assessment of data security and protection training needs across the organisation. |
| 4.2 | Organisation assures good management and maintenance of identity and access control for its networks and information systems |
| 5.1 | Process reviews are held at least once per year where data security is put at risk and following data security incidents. |
| 6.2 | All user devices are subject to anti-virus protections while email services benefit from spam filtering and protection deployed at the corporate gateway. |
| 7.2 | There is an effective test of the continuity plan and disaster recovery plan for data security incidents. |
| 7.3 | You have the capability to enact your incident response plan, including effective limitation of impact on your essential service. During an incident, you have access to timely information on which to base your response decisions. |
| 8.3 | Supported systems are kept up-to-date with the latest security patches. |
| 8.4 | You manage known vulnerabilities in your network and information systems to prevent disruption of the essential service. |
| 9.2 | A penetration test has been scoped and undertaken |
| 10.2 | Basic due diligence has been undertaken against each supplier that handles personal information in accordance with ICO and NHS Digital guidance. |

The scope of this review included only the mandatory elements of the above selected assertions.

## Appendix B: Assurance Definitions and Risk Classifications

| Overall NDG Standard Assurance Rating Classification | Rating Thresholds when only 1 assertion per NDG Standard is in scope | Rating Thresholds when 2 or more assertions are in scope for each NDG Standard. Mean score (Total points divided by the number of in-scope assertions) |
|---|---|---|
| **Substantial** | 1 or less | 1 or less |
| **Moderate** | Greater than 1, less than 10 | Greater than 1, less than 4 |
| **Limited** | Greater than/equal to 10, less than 40 | Greater than/equal to 4, less than 5.9 |
| **Unsatisfactory** | 40 and above | 5.9 and above |

### Overall risk rating across all in-scope standards

| | |
|---|---|
| **Unsatisfactory** | 1 or more Standards is rated as 'Unsatisfactory' |
| **Limited** | No standards are rated as 'Unsatisfactory', but 2 or more are rated as 'Limited' |
| **Moderate** | There are no standards rated as 'Unsatisfactory', and 1 or none rated as 'Limited'. However, not all standards are rated as 'Substantial'. |
| **Substantial** | All of the standards are rated as 'Substantial' |

| Level of deviation from the DSP Toolkit submission and assessment findings | Confidence level | Assurance level |
|---|---|---|
| **High** – the organisation's self-assessment against the Toolkit differs significantly from the Independent Assessment<br><br>For example, the organisation has declared as "Standards Met" or "Standards Exceeded" but the independent assessment has found individual National Data Guardian Standards as 'Unsatisfactory' and the overall rating is 'Unsatisfactory'. | Low | Limited |
| **Medium** - the organisation's self-assessment against the Toolkit differs somewhat from the Independent Assessment<br><br>For example, the Independent Assessor has exercised professional judgement in comparing the self-assessment to their independent assessment and there is a non-trivial deviation or discord between the two. | Medium | Moderate |
| **Low** - the organisation's self-assessment against the Toolkit does not differ / deviates only minimally from the Independent Assessment | High | Substantial |

# A - Summary Scoring

| National Data Guardian (NDG) Standard | Number of DSP Toolkit Assertions Assessed by Independent Assessor | Number of Assertions rated **Critical** and (Weighted Risk Score) | Number of Assertions rated **High** and (Weighted Risk Score) | Number of Assertions rated **Medium** and (Weighted Risk Score) | Number of Assertions rated **Low** **and** (Weighted Risk Score) | Risk Rating Scores [total points/ no. assertions assessed] | Overall Risk Rating at the National Data Guardian Standard level | **Overall risk assessment across all 10 NDG Standards** |
|---|---|---|---|---|---|---|---|---|
| **1. Personal Confidential Data** | **2 assertions assessed out of 8 in this standard** | | | | 2 (2) | | ● Substantial | Substantial |
| **2. Staff Responsibilities** | **1 assertions assessed out of 1 in this standard** | | | | 1 (1) | | ● Substantial | |
| **3. Training** | **1 assertions assessed out of 4 in this standard** | | | | 1 (1) | | ● Substantial | |
| **4. Managing Data Access** | **1 assertions assessed out of 5 in this standard** | | | | 1 (1) | | ● Substantial | |
| **5. Process Reviews** | **1 assertions assessed out of 3 in this standard** | | | | 1 (1) | | ● Substantial | |
| **6. Responding to Incidents** | **1 assertions assessed out of 3 in this standard** | | | | 1 (1) | | ● Substantial | |
| **7. Continuity Planning** | **2 assertions assessed out of 3 in this standard** | | | | 2 (2) | | ● Substantial | |
| **8. Unsupported Systems** | **2 assertions assessed out of 4 in this standard** | | | | 2 (2) | | ● Substantial | |
| **9. IT Protection** | **1 assertions assessed out of 6 in this standard** | | | | 1 (1) | | ● Substantial | |
| **10. Accountable Suppliers** | **1 assertions assessed out of 5 in this standard** | | | | 1 (1) | | ● Substantial | |
| **TOTAL** | **13 of 42** | | | 1 (3) | 12 (12) | - | - | |

# B - Scoring Comparison

National Data Guardian Standard 1: Personal Confidential Data

| Evidence Text Ref. | Evidence Text for Category | Health & Social Care org. DSPT Self-Assessment Rating | Independent Assessor–Evidence Text Risk Rating | Independent Assessor- Assertion Rating<br>*NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.* |
|---|---|---|---|---|
| 1.6.1 | There is an approved procedure that sets out the organisation's approach to data protection by design and by default, which includes pseudonymisation requirements. | Met | Low | Low |
| 1.6.2 | There are technical controls that prevent information from being inappropriately copied or downloaded. | Met | Low | |
| 1.6.3 | There are physical controls that prevent unauthorised access to buildings and locations where personal data are stored or processed. | Met | Low | |
| 1.6.4 | Provide the overall findings of the last data protection by design audit. | Met | Low | |
| 1.8.1 | Does your organisation operate and maintain a data security risk register (including risks from supply chain) which links to the corporate risk framework providing senior visibility? | Met | Low | |
| 1.8.3 | What are your top three data security and protection risks? | Met | Low | |

National Data Guardian Standard 2: Staff Responsibilities

| Evidence Text Ref. | Evidence Text for Category | Health & Social Care org. DSPT Self-Assessment Rating | Independent Assessor–Evidence Text Risk Rating | Independent Assessor- Assertion Rating<br>*NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.* |
|---|---|---|---|---|
| 2.2.1 | Is there a data protection and security induction in place for all new entrants to the organisation? | Met | Low | Low |
| 2.2.2 | Do all employment contracts contain data security requirements? | Met | Low | |

National Data Guardian Standard 3: Training

| Evidence Text Ref. | Evidence Text for Category | Health & Social Care org. DSPT Self-Assessment Rating | Independent Assessor–Evidence Text Risk Rating | Independent Assessor- Assertion Rating<br>*NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.* |
|---|---|---|---|---|
| 3.1.1 | Has an approved organisation-wide data security and protection training needs analysis been completed in the last twelve months? | Met | Low | Low |

National Data Guardian Standard 4: Managing Data Access

| Evidence Text Ref. | Evidence Text for Category | Health & Social Care org. DSPT Self-Assessment Rating | Independent Assessor–Evidence Text Risk Rating | Independent Assessor- Assertion Rating<br>*NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.* |
|---|---|---|---|---|
| 4.2.1 | When was the last audit of user accounts held? | Met | Low | Low |
| 4.2.3 | Logs are retained for a sufficient period, reviewed regularly and can be searched to identify malicious activity. | Met | Low | |
| 4.2.5 | Are unnecessary user accounts removed or disabled? | Met | Low | |

National Data Guardian Standard 5: Process Reviews

| Evidence Text Ref. | Evidence Text for Category | Health & Social Care org. DSPT Self-Assessment Rating | Independent Assessor–Evidence Text Risk Rating | Independent Assessor- Assertion Rating<br>*NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.* |
|---|---|---|---|---|
| 5.1.1 | Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security incident, with findings acted upon. | Met | Low | Low |
| 5.1.2 | Provide summary details of process reviews held to identify and manage problem processes that cause security breaches. | Met | Low | |

National Data Guardian Standard 6: Responding to Incidents

| Evidence Text Ref. | Evidence Text for Category | Health & Social Care org. DSPT Self-Assessment Rating | Independent Assessor–Evidence Text Risk Rating | Independent Assessor- Assertion Rating<br>*NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.* |
|---|---|---|---|---|
| 6.2.2 | Number of alerts recorded by the antivirus/anti-malware tool in the last three months. | Met | Low | Low |
| 6.2.3 | Has antivirus/anti-malware software been installed on all computers that are connected to or capable of connecting to the Internet? | Met | Low | |
| 6.2.4 | Antivirus/anti-malware is kept continually up to date. | Met | Low | |
| 6.2.5 | Antivirus/anti-malware software scans files automatically upon access. | Met | Low | |
| 6.2.6 | Connections to malicious websites on the Internet are prevented. | Met | Low | |

| | | | | |
|---|---|---|---|---|
| 6.2.10 | Does the organisation maintain a list of approved applications, and are users prevented from installing any application that is unsigned or has an invalid signature? | Met | Low | |
| 6.2.11 | You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) for your organisation's domains to make email spoofing difficult. | Met | Low | |
| 6.2.12 | You have implemented spam and malware filtering, and enforce DMARC on inbound email. | Met | Low | |
| | | | | |
| National Data Guardian Standard 7: Continuity Planning | | | | |
| **Evidence Text Ref.** | **Evidence Text for Category** | **Health & Social Care org. DSPT Self-Assessment Rating** | **Independent Assessor–Evidence Text Risk Rating** | **Independent Assessor- Assertion Rating** *NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.* |
| 7.2.1 | Explain how your data security incident response and management plan has been tested to ensure all parties understand their roles and responsibilities as part of the plan. | Met | Low | Low |
| 7.2.4 | From the business continuity exercise, explain what issues and actions were documented, with names of actionees listed against each item. | Met | Low | |
| 7.3.1 | On discovery of an incident, mitigating measures shall be assessed and applied at the earliest opportunity, drawing on expert advice where necessary. | Met | Low | |
| 7.3.2 | All emergency contacts are kept securely, in hardcopy and are up-to-date. | Met | Low | |
| 7.3.4 | Suitable backups of all important data and information needed to recover the essential service are made, tested, documented and routinely reviewed. | Met | Low | |
| 7.3.5 | When did you last successfully restore from backup? | Met | Low | |
| 7.3.6 | Are your backups kept separate from your network ('offline'), or in a cloud service designed for this purpose | Met | Low | |
| | | | | |
| National Data Guardian Standard 8: Unsupported Systems | | | | |
| **Evidence Text Ref.** | **Evidence Text for Category** | **Health & Social Care org. DSPT Self-Assessment Rating** | **Independent Assessor–Evidence Text Risk Rating** | **Independent Assessor- Assertion Rating** *NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.* |
| 8.3.1 | How do your systems receive updates and how often? | Met | Low | Low |
| 8.3.2 | How often, in days, is automatic patching typically being pushed out to remote endpoints? | Met | Low | |
| 8.3.3 | There is a documented approach to applying security updates (patches) agreed by the SIRO. | Met | Low | |
| 8.3.4 | Where a security patch has been classed as critical or high-risk vulnerability it is applied within 14 days, or the risk has been assessed, documented, accepted and signed off by the SIRO with an auditor agreeing a robust risk management process has been applied. | Met | Low | |
| 8.4.1 | Is all your infrastructure protected from common cyber-attacks through secure configuration and patching? | Met | Low | |
| 8.4.2 | All infrastructure is running operating systems and software packages that are patched regularly, and as a minimum in vendor support. | Met | Low | |
| | | | | |
| National Data Guardian Standard 9: IT Protection | | | | |
| **Evidence Text Ref.** | **Evidence Text for Category** | **Health & Social Care org. DSPT Self-Assessment Rating** | **Independent Assessor–Evidence Text Risk Rating** | **Independent Assessor- Assertion Rating** *NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.* |
| 9.2.1 | The annual IT penetration testing is scoped in negotiation between the SIRO, business and testing team including a vulnerability scan and checking that all networking components have had their default passwords changed to a high strength password. | Met | Low | Low |
| 9.2.2 | The date the penetration test and vulnerability scan was undertaken. | Met | Low | |
| | | | | |
| National Data Guardian Standard 10: Accountable suppliers | | | | |
| **Evidence Text Ref.** | **Evidence Text for Category** | **Health & Social Care org. DSPT Self-Assessment Rating** | **Independent Assessor–Evidence Text Risk Rating** | **Independent Assessor- Assertion Rating** *NB. Based on the Evidence Text Ratings and the Independent Assessor's knowledge of the relative importance of the controls in question and the mitigating controls in place, he/she uses professional judgement to assign an Assertion Risk Rating.* |
| 10.2.1 | Your organisation ensures that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification. | Met | Low | Low |
| 10.2.2 | Your organisation determines, as part of its risk assessment, whether the supplier certification is sufficient assurance. | Met | Low | |
| 10.2.4 | Where services are outsourced (for example by use of cloud infrastructure or services), the organisation understands and accurately records which security related responsibilities remain with the organisation and which are the supplier's responsibility. | Met | Low | |

# D - Scoring Guide - Impact

| Impact rating | Assessment rationale |
|---|---|
| **Critical** | A **Critical Impact Finding** could apply to Health and Social Care organisations that use extremely complex technologies to deliver multiple services or process large volumes of patient data, including processing for other organisations. Many of the services are at the highest level of risk, including those offered to other organisations. New and emerging technologies are utilised across multiple delivery channels. The organisation is responsible for/ maintains nearly all connection types to transfer/store/process personal, patient identifiable and/or business-critical data with customers and third parties. A Critical finding that could have a:<br>•Critical impact on operational performance or the ability to deliver services / care*;* or<br>•Critical monetary or financial statement impact; or<br>•Critical breach in laws and regulations that could result in material fines or consequences*;* or<br>•Critical impact on the reputation or brand of the organisation which could threaten its future viability. |
| **Significant** | A **Significant Impact Finding** could apply to a Health and Social Care organisation that use complex technology in terms of scope and sophistication. The organisation may offer high-risk products and services that may include emerging technologies. The organisation is responsible for/ maintains the largest proportion of connection types to transfer/store/process personal, patient identifiable or business-critical data with customers and third parties; other organisations and/or third-parties are responsible for/maintain a low proportion of connection types. A Significant finding that could have a:<br>•Significant impact on operational performance*;* or<br>•Significant monetary or financial statement impact; or<br>•Significant breach in laws and regulations resulting in large fines and consequences*;* or<br>•Significant impact on the reputation or brand of the organisation*.* |
| **Moderate** | A **Moderate Impact Finding** could apply to a Health and Social Care organisation that uses technology which may be somewhat complex in terms of volume and sophistication. The organisation is responsible for/maintains a some connection types to transfer/store/process personal, patient identifiable and/or business-critical data with customers and third parties; other organisations and/or third-parties are responsible for/maintain a most of the organisation's connection types. A Moderate finding that could have a:<br>•Moderate impact on the organisation's operational performance; or<br>•Moderate monetary or financial statement impact; or<br>•Moderate breach in laws and regulations with moderate consequences; or<br>•Moderate impact on the reputation of the organisation. |
| **Minor** | A **Minor Impact Finding** could apply to a Health and Social Care organisation with limited complexity in terms of the technology it uses. It offers a limited variety of less risky products and services. The institution primarily uses established technologies. It is responsible for/maintains minimal numbers of connection types to transfer/store/process personal, patient identifiable or business-critical data too customers and third parties; other organisations and/or third-parties are largely responsible for/maintain connection types. A Minor finding that could have a:<br>•Minor impact on the organisation's operational performance; or<br>•Minor monetary or financial statement impact; or<br>•Minor breach in laws and regulations with limited consequences; or<br>•Minor impact on the reputation of the organisation. |
| **Very Low / Insignificant** | A **Low Impact Finding** could apply to a Health and Social Care organisation that has very limited use of technology. The variety of products and services are limited and the organisation has a small geographic footprint with few employees. It is responsible for/maintains no connection types to transfer/store/process personal, patient identifiable or business-critical data too customers and third parties. A Low finding that could have a:<br>•Insignificant impact on the organisation's operational performance; or<br>•Insignificant monetary or financial statement impact; or<br>•Insignificant breach in laws and regulations with little consequence; or<br>•Insignificant impact on the reputation of the organisation. |

# E - Scoring Guide - Likelihood

| Likelihood rating | Assessment rationale |
|---|---|
| **>80%** | > 80% likely to happen in the next 12 months |
| **60% - 80%** | 60% - 80% likely to happen in the next 12 months |
| **40% - 60%** | 40% - 60% likely to happen in the next 12 months |
| **20% - 40%** | 20% - 40% likely to happen in the next 12 months |
| **< 20%** | Low likelihood to happen in the next 12 months |

# F - Scoring Guide - Risk Rating

| | Impact rating | | | | |
|---|---|---|---|---|---|
| Likelihood rating (in next 12 months) | Critical | Significant | Moderate | Minor | Very Low |
| >80% | Critical | High | Medium | Low | Low |
| 60% - 80% | High | Medium | Medium | Low | Low |
| 40% - 60% | Medium | Medium | Low | Low | Low |
| 20% - 40% | Medium | Low | Low | Low | Not reportable |
| < 20% | Low | Low | Low | Not reportable | Not reportable |

| Rating | Points for each Assertion |
|---|---|
| Critical | 40 |
| High | 10 |
| Medium | 3 |
| Low | 1 |